(3)

35.C15052

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	:	Examiner: Not Assigned
MITSURU MAEDA	)	
	:	Group Art Unit: 2132
Application No.: 09/761,721	)	
	:	
Filed: January 18, 2001	)	
	:	
For: INFORMATION PROCESSING APPARATUS AND METHOD	)	May 2, 2001
	:	

Commissioner for Patents
Washington, D.C. 20231

CLAIM TO PRIORITY

Sir:

Applicant hereby claims priority under the International Convention and all rights to which he is entitled under 35 U.S.C. § 119 based upon the following Japanese Priority Application:

JAPAN	2000-012965	January 21, 2000

A certified copy of the priority document is enclosed.

Applicant's undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010 All correspondence should continue to be directed to our address given below.

Respectfully submitted,

Attorney for Applicant
Brian L. Klock
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

BLK/dc

本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月２１日

出願番号
Application Number: 特願２０００－０１２９６５

出願人
Applicant (s): キヤノン株式会社

２００１年　２月　９日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３００６２７５

【書類名】　特許願
【整理番号】　4144147
【提出日】　平成12年 1月21日
【あて先】　特許庁長官　近藤　隆彦　殿
【国際特許分類】　H04L　9/00
【発明の名称】　画像処理装置及びその方法並びに記憶媒体
【請求項の数】　42
【発明者】
　【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
　【氏名】　前田　充
【特許出願人】
　【識別番号】　000001007
　【住所又は居所】　東京都大田区下丸子３丁目３０番２号
　【氏名又は名称】　キヤノン株式会社
　【代表者】　御手洗　冨士夫
　【電話番号】　03-3758-2111
【代理人】
　【識別番号】　100090538
　【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
　【弁理士】
　【氏名又は名称】　西山　恵三
　【電話番号】　03-3758-2111
【選任した代理人】
　【識別番号】　100096965
　【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
　【弁理士】

【氏名又は名称】　内尾　裕一

【電話番号】　03-3758-2111

【選任した代理人】

【識別番号】　100110009

【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

【弁理士】

【氏名又は名称】　青木　康

【電話番号】　03-3758-2111

【選任した代理人】

【識別番号】　100069877

【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

【弁理士】

【氏名又は名称】　丸島　儀一

【電話番号】　03-3758-2111

【手数料の表示】

【予納台帳番号】　011224

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9908388

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　画像処理装置及びその方法並びに記憶媒体

【特許請求の範囲】

【請求項１】　画像データを入力する入力手段と、

前記画像データを保護するためのセキュリティデータを生成する生成手段と、

前記画像データを符号化し、符号化データを生成する符号化手段と、

前記セキュリティデータに従ってセキュリティが設定される区間の符号化データから一意に決定される所定符号を抽出する抽出手段と、

前記所定符号に前記セキュリティデータを重畳する重畳手段と、

前記セキュリティが設定された区間において前記所定符号を除いた前記符号化データにスクランブルを施すスクランブル手段と、

前記重畳手段によって処理された所定符号と前記スクランブル手段によって処理された符号化データとを出力する出力手段とを有することを特徴とする画像処理装置。

【請求項２】　前記セキュリティデータは前記スクランブル手段に使用されるキー情報を含むことを特徴とする請求項１に記載の画像処理装置。

【請求項３】　前記セキュリティデータは認証のための情報を含むことを特徴とする請求項１又は２に記載の画像処理装置。

【請求項４】　前記符号化手段はMPEG－4のビットストリームを生成することを特徴とする請求項１～３のいずれか１項に記載の画像処理装置。

【請求項５】　前記セキュリティに関する情報を示すIPMPデータを生成するIPMP符号化手段を有し、前記出力手段は前記IPMP符号化手段によって生成されたIPMPデータを出力することを特徴とする請求項４に記載の画像処理装置。

【請求項６】　前記セキュリティデータを暗号化する暗号化手段を有し、前記重畳手段は前記暗号化手段によって暗号化されたセキュリティデータを重畳することを特徴とする請求項１～５のいずれか１項に記載の画像処理装置。

【請求項７】　前記抽出手段によって抽出される符号はスタートコードであることを特徴とする請求項１～６のいずれか１項に記載の画像処理装置。

【請求項８】　画像符号化データから一意に決定される所定符号にセキュリ

データが適応的に重畳され、前記所定符号を除いた画像符号化データに前記セキュリティデータに応じて適応的にスクランブル処理されている符号化データを入力する入力手段と、

前記符号化データから前記所定符号が存在する位置にある符号を抽出する符号抽出手段と、

前記抽出された符号からセキュリティデータを検出する検出手段と、

前記検出手段の検出結果に応じて前記符号化データをデスクランブル処理するデスクランブル手段と、

前記デスクランブル手段によってデスクランブル処理された画像符号化データを復号化する復号化手段とを有することを特徴とする画像処理装置。

【請求項９】　前記セキュリティデータには認証判定のために認証データが含まれており、前記認証データに応じて認証判定を行なう認証手段を有することを特徴とする請求項８に記載の画像処理装置。

【請求項１０】　前記デスクランブル手段は前記認証手段の判定結果に応じてスクランブル処理された符号化データをデスクランブルすることを特徴とする請求項８に記載の画像処理装置。

【請求項１１】　前記セキュリティデータは暗号化されており、前記暗号化されたセキュリティデータを解読する解読手段を有することを特徴とする請求項８～１０のいずれか１項に記載の画像処理装置。

【請求項１２】　前記画像符号化データはMPEG-4のビットストリームデータであることを特徴とする請求項８に記載の画像処理装置。

【請求項１３】　前記入力手段はセキュリティに関する情報を示すIPMPデータを入力することを特徴とする請求項１２に記載の画像処理装置。

【請求項１４】　前記IPMPデータには認証判定のために認証データが含まれており、前記認証データに応じて認証判定を行なう認証手段を有することを特徴とする請求項１３に記載の画像処理装置。

【請求項１５】　前記デスクランブル手段は前記認証手段の判定結果に応じてスクランブル処理された符号化データをデスクランブルすることを特徴とする請求項１４に記載の画像処理装置。

【請求項１６】　前記セキュリティデータは暗号化されており、前記暗号化されたセキュリティデータを前記認証手段の判定結果に応じて解読する解読手段を有することを特徴とする請求項１４又は１５に記載の画像処理装置。

【請求項１７】　前記所定符号とはスタートコードであることを特徴とする請求項８～１６のいずれか１項に記載の画像処理装置。

【請求項１８】　画像データを入力する入力工程と、

前記画像データを保護するためのセキュリティデータを生成する生成工程と、

前記画像データを符号化し、符号化データを生成する符号化工程と、

前記セキュリティデータに従ってセキュリティが設定される区間の符号化データから一意に決定される所定符号を抽出する抽出工程と、

前記所定符号に前記セキュリティデータを重畳する重畳工程と、

前記セキュリティが設定された区間において前記所定符号を除いた前記符号化データにスクランブルを施すスクランブル工程と、

前記重畳処理された所定符号と前記スクランブル処理された符号化データとを出力する出力工程とを有することを特徴とする画像処理方法。

【請求項１９】　前記セキュリティデータは前記スクランブル工程に使用されるキー情報を含むことを特徴とする請求項１８に記載の画像処理方法。

【請求項２０】　前記セキュリティデータは認証のための情報を含むことを特徴とする請求項１８又は１９に記載の画像処理方法。

【請求項２１】　前記符号化工程はMPEG－4のビットストリームを生成することを特徴とする請求項１８～２０のいずれか１項に記載の画像処理方法。

【請求項２２】　前記セキュリティに関する情報を示すIPMPデータを生成するIPMP符号化工程を有し、前記出力工程は前記IPMP符号化工程によって生成されたIPMPデータを出力することを特徴とする請求項２１に記載の画像処理方法。

【請求項２３】　前記セキュリティデータを暗号化する暗号化工程を有し、前記重畳工程は前記暗号化工程によって暗号化されたセキュリティデータを重畳することを特徴とする請求項１８～２２のいずれか１項に記載の画像処理方法。

【請求項２４】　前記抽出工程によって抽出される符号はスタートコードであることを特徴とする請求項１８～２３のいずれか１項に記載の画像処理方法。

【請求項２５】　画像符号化データから一意に決定される所定符号にセキュリデータが適応的に重畳され、前記所定符号を除いた画像符号化データに前記セキュリティデータに応じて適応的にスクランブル処理されている符号化データを入力する入力工程と、

前記符号化データから前記所定符号が存在する位置にある符号を抽出する符号抽出工程と、

前記抽出された符号からセキュリティデータを検出する検出工程と、

前記検出工程の検出結果に応じて前記符号化データをデスクランブル処理するデスクランブル工程と、

前記デスクランブル処理された画像符号化データを復号化する復号化工程とを有することを特徴とする画像処理方法。

【請求項２６】　前記セキュリティデータには認証判定のために認証データが含まれており、前記認証データに応じて認証判定を行なう認証工程を有することを特徴とする請求項２５に記載の画像処理方法。

【請求項２７】　前記デスクランブル工程は前記認証工程の判定結果に応じてスクランブル処理された符号化データをデスクランブルすることを特徴とする請求項２６に記載の画像処理方法。

【請求項２８】　前記セキュリティデータは暗号化されており、前記暗号化されたセキュリティデータを解読する解読工程を有することを特徴とする請求項２５～２７のいずれか１項に記載の画像処理方法。

【請求項２９】　前記画像符号化データはMPEG-4のビットストリームデータであることを特徴とする請求項２５に記載の画像処理方法。

【請求項３０】　前記入力工程はセキュリティに関する情報を示すIPMPデータを入力することを特徴とする請求項２９に記載の画像処理方法。

【請求項３１】　前記IPMPデータには認証判定のために認証データが含まれており、前記認証データに応じて認証判定を行なう認証工程を有することを特徴とする請求項３０に記載の画像処理方法。

【請求項３２】　前記デスクランブル工程は前記認証工程の判定結果に応じてスクランブル処理された符号化データをデスクランブルすることを特徴とする

請求項３１に記載の画像処理方法。

【請求項３３】　前記セキュリティデータは暗号化されており、前記暗号化されたセキュリティデータを前記認証工程の判定結果に応じて解読する解読工程を有することを特徴とする請求項３１又は３２に記載の画像処理方法。

【請求項３４】　前記所定符号とはスタートコードであることを特徴とする請求項２５～３３のいずれか１項に記載の画像処理方法。

【請求項３５】　階層構造を形成する画像符号化データを入力する入力工程と、

前記画像符号化データから所定層の先頭を示す所定コードを抽出する抽出工程と、

前記抽出工程によって抽出された所定コードに画像保護のためのセキュリティデータを重畳する重畳工程とを有することを特徴とする画像処理方法。

【請求項３６】　前記セキュリティデータに応じて前記画像符号化データに暗号化を行なう暗号化工程とを有することを特徴とする請求項３５に記載の画像処理方法。

【請求項３７】　階層構造を形成する画像符号化データに対して、所定階層の先頭を示す所定コードにセキュリティデータを重畳した符号化データを入力する入力工程と、

前記符号化データから前記所定コードが存在する位置にある符号を抽出する抽出工程と、

前記抽出された符号から前記セキュリティデータを検出する検出工程と、

前記検出工程の検出結果に応じて前記符号化データを復号化する復号化工程とを有することを特徴とする画像処理方法。

【請求項３８】　前記符号化データは暗号化されており、前記復号化工程には前記暗号化を解読する工程が含まれていることを特徴とする請求項３７に記載の画像処理方法。

【請求項３９】　請求項１８～２４のいずれか1項に記載の画像処理方法を実行する制御プログラムを記憶したコンピュータにより読取り可能な記憶媒体。

【請求項４０】　請求項２５～３４のいずれか1項に記載の画像処理方法を

実行する制御プログラムを記憶したコンピュータにより読取り可能な記憶媒体。

【請求項４１】　請求項３５又は３６に記載の画像処理方法を実行する制御プログラムを記憶したコンピュータにより読取り可能な記憶媒体。

【請求項４２】　請求項３７又は３８に記載の画像処理方法を実行する制御プログラムを記憶したコンピュータにより読取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、画像処理装置及びその方法並ぶにその画像処理プログラムが記録されたコンピュータにより読取り可能な記憶媒体に関し、特に画像の著作権等の保護を行うための画像処理に関するものである。

【０００２】

【従来の技術】

従来、動画像の符号化方式として、フレーム内符号化方式であるMotion JPEGやDigital Video等の符号化方式や、フレーム間予測符号化を用いたH.２６１、H.２６３、MPEG-１、MPEG-２等の符号化方式が知られている。これらの符号化方式はＩＳＯ(International Organization for Standardization：国際標準化機構)やＩＴＵ（International Telecommunication Union：国際電気通信連合）によって国際標準化されている。前者の符号化方式はフレーム単位で独立に符号を行うもので、フレームの管理がしやすいため、動画像の編集や特殊再生が必要な装置に最適である。また、後者の符号化方式はフレーム間予測を用いるため、符号化効率が高いという特徴を持っている。

【０００３】

さらにコンピュータ・放送・通信など多くの領域で利用できる、汎用的な次世代マルチメディア符号化規格としてMPEG-４の国際標準化作業が進められている。

【０００４】

また、上述したようなディジタル符号化規格の普及に伴い、コンテンツ業界からは著作権保護の問題が強く提起されるようになってきた。即ち、著作権が保護

されることが十分に保証されていない規格に対しては、安心して優良なコンテンツを提供することができない、という問題が生じている。

【０００５】

このため、MPEG-４ではその標準の中で著作権の保護を行うようにIPMP（Intellectual Property Management & Protection)の機能を盛り込むべくパート1であるSystems（ISO 14496－1）にデータが記載できるようになった。詳細はISO 14496－1を参照されたい。

【０００６】

図１１にMPEG-４の符号化データの構成例を示す。

【０００７】

図１１において、１０１０はBIFS符号化データであり、パート1に記載されているオブジェクトの合成方法や各オブジェクトの同期等の情報が符号化されたものである。１０１１はIPMP符号化データであり、各ビットストリームのセキュリティに関する情報が記載されている。１０１２は動画像の画像データの符号化結果であるビデオ符号化データである。１０１３は動画像に付随するオーディオデータの符号化結果であるオーディオ符号化データである。

【０００８】

IPMP符号化データ１０１１に記載されている情報の例を図１２に示す。

【０００９】

まず、セキュリティが設定された符号化データを示す情報が含まれている。図１２ではビデオ符号化データ１０１２である。続いてこの符号化データの復号を許可できるかどうかを判定するための認証データが入っている。図１２では「nonac」が認証データである。一般にこのデータは暗号化されている。本例では認証データ「canon」を逆転させた状態で暗号化されていることを示している。

【００１０】

さらに、ビデオに対してはセキュリティをシーケンスの一部に施すためにその保護するフレームの番号とそのフレームのデータがスクランブルによって暗号化されている場合には解読のためのキーを暗号化した情報が記載されている。図１２ではビデオ符号化データの中でフレーム番号1から100までが解読キー「key」

で、フレーム番号1000から1260までを解読キー「maeda」でデスクランブルできることを示している。これらが符号化されたものがIPMP符号化データ１０１１である。

ビデオ符号化データ１０１２はIPMP符号化データがセキュリティを施すフレームに対してスクランブルを施すことでセキュリティを実現している。

【００１１】

このような符号化データを復号する復号装置の例を図１０に示す。

【００１２】

図１０において、１０００は動画像データの符号化データのうち、IPMP符号化データ１０１１とビデオ符号化データ１０１２を入力する入力端子である。１００１は入力された符号化データをIPMP符号化データ１０１１とビデオ符号化データ１０１２に分離する分離器である。１００２はバッファであり、分離器１００１で分離されたビデオ符号化データ１０１２を各フレーム単位で格納する。

【００１３】

１００３はIPMP符号化データを復号するIPMP復号器である。１００４ は認証を確認する認証器である。１００５と１００７はセレクタであり、認証器１００４の出力にしたがって入出力先を変更する。１００６はデスクランブラである。１００８はビデオの符号化データを復号し、画像データを再生するビデオ復号器である。１００９は再生された画像データを出力する出力端子である。

【００１４】

上述のように構成された復号装置の動作を以下に説明する。

【００１５】

入力端子１０００から最初にIPMP符号化データ１０１１が入力される。分離器１００１はこの符号化データをIPMP復号器１００３に入力する。IPMP復号器１００３はIPMP符号化データ１０１１を復号し、認証データ、セキュリティの対象となっているフレーム番号やデスクランブルのためのキーを復号する。

【００１６】

認証データは認証器１００４に入力され、あらかじめ登録された認証データと比較され、認証が正しくなければ常にセレクタ１００５とセレクタ１００７を直

結し、デスクランブラ１００６を介さないように指示する。認証が正しければセレクタ１００５、１００７がIPMP復号器１００３の指示に従ってデスクランブラ１００６を経由するか、しないかを選択する。

【００１７】

この場合では、IPMP復号器１００３がセキュリティを施すフレームの符号化データと認識した場合、セレクタ１００５、１００７にデスクランブラ１００６を経由するように指示を行う。それ以外の場合はデスクランブル１００６を経由しないように指示する。

【００１８】

すなわち、セレクタ１００５、１００７は認証器１００４が正しく認証できなかった場合、および正しく認証できた場合でIPMP復号器１００３がデスクランブラ１００６を経由しない場合はお互いを入出力として選択する。また、正しく認証が行え、IPMP復号器１００３がセキュリティを施すフレームの符号化データと認識した場合はデスクランブラ１００６を経由するように選択する。

【００１９】

従って、正しく認証が行えた場合、ビデオ復号器１００８はセキュリティの施されていないフレームに加えてセキュリティの施されたフレームもデスクランブル処理をデスクランブラ１００６で行っているため、正しい画像を再生することができる。正しく認証できない場合はスクランブルが施された符号化データがビデオ復号器１００８に入力され、ビデオ復号器１００８は正しく復号できないため再生画像は生成されない。

【００２０】

【発明が解決しようとする課題】

しかしながら、このような構成では、ビデオデータを編集する際に必ずIPMP符号化データを編集する必要が生じ、処理が煩雑になる。たとえば別なシーケンスと組み合わせて１つのビットストリームを生成しようとするとフレーム番号が変わり、IPMP符号化データも変更する必要が出る。また、スクランブルのためのキー情報をセキュリティの対象となるデータと別に用意する必要があり、冗長な情報を付加することになる。

【００２１】

従って、本発明は前記課題を考慮して画像の著作権保護のために画像データを好適に処理する画像データ処理装置及び方法、画像データ処理プログラムが記録されたコンピュータ可読記録媒体を提供することを目的としている。

【００２２】

【課題を解決するための手段】

上記目的を達成するための本発明による画像処理装置は、画像データを入力する入力手段と、前記画像データを保護するためのセキュリティデータを生成する生成手段と、前記画像データを符号化し、符号化データを生成する符号化手段と、前記セキュリティデータに従ってセキュリティが設定される区間の符号化データから一意に決定される所定符号を抽出する抽出手段と、前記所定符号に前記セキュリティデータを重畳する重畳手段と、前記セキュリティが設定された区間において前記所定符号を除いた前記符号化データにスクランブルを施すスクランブル手段と、前記重畳手段によって処理された所定符号と前記スクランブル手段によって処理された符号化データとを出力する出力手段とを有することを特徴とする。

【００２３】

また、上記目的を達成するために本発明の他の態様による画像処理装置は、画像符号化データから一意に決定される所定符号にセキュリデータが適応的に重畳され、前記所定符号を除いた画像符号化データに前記セキュリティデータに応じて適応的にスクランブル処理されている符号化データを入力する入力手段と、前記符号化データから前記所定符号が存在する位置にある符号を抽出する符号抽出手段と、前記抽出された符号からセキュリティデータを検出する検出手段と、前記検出手段の検出結果に応じて前記符号化データをデスクランブル処理するデスクランブル手段と、前記デスクランブル手段によってデスクランブル処理された画像符号化データを復号化する復号化手段とを有することを特徴とする。

【００２４】

また、上記目的を達成するために本発明の他の態様による画像処理方法は、画像データを入力する入力工程と、前記画像データを保護するためのセキュリティ

データを生成する生成工程と、前記画像データを符号化し、符号化データを生成する符号化工程と、前記セキュリティデータに従ってセキュリティが設定される区間の符号化データから一意に決定される所定符号を抽出する抽出工程と、前記所定符号に前記セキュリティデータを重畳する重畳工程と、前記セキュリティが設定された区間において前記所定符号を除いた前記符号化データにスクランブルを施すスクランブル工程と、前記重畳処理された所定符号と前記スクランブル処理された符号化データとを出力する出力工程とを有することを特徴とする。

【００２５】

また、上記目的を達成するために本発明の他の態様による画像処理方法は、画像符号化データから一意に決定される所定符号にセキュリデータが適応的に重畳され、前記所定符号を除いた画像符号化データに前記セキュリティデータに応じて適応的にスクランブル処理されている符号化データを入力する入力工程と、前記符号化データから前記所定符号が存在する位置にある符号を抽出する符号抽出工程と、前記抽出された符号からセキュリティデータを検出する検出工程と、前記検出工程の検出結果に応じて前記符号化データをデスクランブル処理するデスクランブル工程と、前記デスクランブル処理された画像符号化データを復号化する復号化工程とを有することを特徴とする。

【００２６】

また、上記目的を達成するために本発明の他の態様による画像処理方法は、階層構造を形成する画像符号化データを入力する入力工程と、前記画像符号化データから所定層の先頭を示す所定コードを抽出する抽出工程と、前記抽出工程によって抽出された所定コードに画像保護のためのセキュリティデータを重畳する重畳工程とを有することを特徴とする。

【００２７】

また、上記目的を達成するために本発明の他の態様による画像処理方法は、階層構造を形成する画像符号化データに対して、所定階層の先頭を示す所定コードにセキュリティデータを重畳した符号化データを入力する入力工程と、前記符号化データから前記所定コードが存在する位置にある符号を抽出する抽出工程と、前記抽出された符号から前記セキュリティデータを検出する検出工程と、前記検

出工程の検出結果に応じて前記符号化データを復号化する復号化工程とを有することを特徴とする。

【００２８】

【発明の実施の形態】

以下、本発明の実施例を、図面を用いて詳細に説明する。

【００２９】

＜第１実施例＞

図１は、本発明の第１の実施例としての画像データ処理装置の構成を示すブロック図である。尚、本実施例では、ビデオの符号化方式としてMPEG-4を用いた場合について説明する。ただし、これに限定されるものではなく、H.261、H.263、MPEG-１、MPEG-2等およびその他の符号化方式であってももちろんかまわない。

【００３０】

図１において、１００は画像データを入力する入力端子であり、１フレームずつ画像データを入力する。１０１はMPEG-4符号化方式で動画像を符号化するビデオ符号化器である。１０４は動画像を保護するセキュリティの設定を行うセキュリティ設定器である。１０２、１１２はセレクタであり、セキュリティ設定器１０４の指示で入出力先を選択する。

【００３１】

１０３はバッファであり、符号化データを一時格納する。１０５は符号化データの中からスタートコードを検出する検出器である。１０８はセキュリティの保護を行うために符号化データに対してスクランブルを行うキーを生成するキー生成器である。１１０はセキュリティの解除に必要な認証のデータを設定する認証設定器である。

【００３２】

１０９は暗号化器であり、入力されたデータを所定の暗号方式で暗号化して出力する。１０６はスタートコードに暗号化されたデータを重畳する暗号重畳器である。１０７はスクランブラであり、前述のキーにしたがってスクランブルを行う。１１１は合成器であり、暗号重畳器１０６の出力とスクランブラ１０７の出力を合成する。１１３は外部からオーディオ符号化データを入力する入力端子で

ある。

【００３３】

１１４はビデオのフレーム単位で音声を多重化する多重化器である。１１５は生成された符号化データを出力する出力端子である。

【００３４】

上述のように構成された画像データ処理装置の動作を以下で説明する。

【００３５】

まず、操作者は、セキュリティ設定器１０４で著作権を保護するデータの区間を決定し、設定する。ここで説明を容易にするため、フレーム番号１から始まる画像データのシーケンスにおいて、フレーム番号ｎからフレーム番号（ｎ＋ｍ）に対してセキュリティを施すこととする。

【００３６】

入力端子１００からフレーム単位で画像データが入力され、ビデオ符号化器１０１で符号化され、フレーム単位でセレクタ１０２に入力される。セキュリティ設定器１０４でセキュリティを施さないフレーム（フレーム番号１から（ｎ－１）、またはフレーム番号（ｎ＋ｍ＋１）以上）としていた場合、セレクタ１０２の出力およびセレクタ１１２の入力をバッファ１０３とする。この場合、符号化データにはスクランブル等のセキュリティは施されず、出力端子１１５から出力される。

【００３７】

一方、セキュリティ設定器１０４でセキュリティを施すフレーム（フレーム番号ｎから（ｎ＋ｍ））としていた場合について述べる。セキュリティ設定器１０４はキー生成器１０８に該当するフレームのスクランブルのときに使用するキーを生成させる。生成されたキーはスクランブラ１０７と暗号化器１０９に入力される。

【００３８】

また、認証設定器１１０は認証に必要なデータたとえばパスワードを設定し、暗号化器１０９に入力する。暗号化器１０９はこれらを所定の暗号化方式で暗号化し、３２ビット以下の暗号データを生成する。本実施例では２３ビットの暗号

データαを生成するものとする。

【００３９】

また、セレクタ１０２は出力先をスタートコード検出器１０５とし、セレクタ１１２は入力先を合成器１１１とする。従って、セレクタ１０２に入力された符号化データはスタートコード検出器１０５に入力される。

【００４０】

MPEG-4で使用されるスタートコードは表1に示すとおりである。

【００４１】

【表１】

符号名	符号（16進）
video_object_start_code	00000100～0000011F
video_object_layer_start_code	00000120～0000012F
Reserved	00000130～000001AF
visual_object_sequence_start_code	000001B0
visual_object_sequence_end_code	000001B1
user_data_start_code	000001B2
group_of_vop_start_code	000001B3
video_session_error_code	000001B4
visual_object_start_code	000001B5
vop_start_code	000001B6
Reserved	000001B7～000001B9
face_object_start_code	000001BA
face_object_plane_start_code	000001BB
mesh_object_start_code	000001BC
mesh_object_plane_start_code	000001BD
still_texture_object_start_code	000001BE
texture_spatial_layer_start_code	000001BF
texture_snr_layer_start_code	000001C0
Reserved	000001C1－C5
System start codes (see note)	000001C6～000001FF

【００４２】

本実施例では、スタートコード検出器１０５はVOPスタートコード(vop_start_code）を検出する。それ以外の符号化データはスクランブラ１０７に入力される。

【００４３】

検出されたVOPスタートコードは暗号重畳器１０６に入力される。暗号重畳器１０６では暗号データαを９ビット左にシフトし、VOPスタートコードと論理的

排他和をとる。例えば、暗号データαが１６進で“7234A”であったとき暗号重畳器１０６の出力は“E4715B6”となる。

【００４４】

キー生成器１０８で生成されたキーはスクランブラ１０７に入力され、このキーを使ってスタートコードを除く符号化データに対してスクランブルを施し、合成器１１１に入力される。合成器１１１はVOPスタートコードに暗号データαを重畳した結果を先頭に、スクランブルが施された符号化データと合成する。

【００４５】

入力端子１１３からは外部で符号化されたオーディオ符号化データが入力され、フレーム単位でセレクタ１１２から出力されるビデオ符号化データと多重化してパケット化して出力端子１１５から出力される。

【００４６】

このような一連の符号化、暗号化、選択処理によりセキュリティを施した符号化データを、冗長を生じることなく実施できる。

【００４７】

なお、本実施例においては検出する一意の符号としてスタートコードを選択したが、これに限定されず、先頭から固定長または可変長でも一意に符号が検出できる符号であればいかなる符号を検出してもかまわない。

【００４８】

また、本実施例では検出するスタートコードとしてVOPスタートコードを検出したがこれに限定されず、上位のスタートコードを検出してももちろんかまわない。たとえばレイヤー単位でセキュリティを制御する場合はVOLスタートコード、シークエンス単位で制御する場合はVOSスタートコードに対してキーや認証情報の重畳を行えばよい。

【００４９】

＜第２実施例＞

図２は、本発明の第２の実施例としての画像データ処理装置の構成を示すブロック図である。

【００５０】

２００は符号化データを入力する入力端子である。本実施例では第１実施例で生成された符号化データを処理するものとし、図１の出力端子１１５に接続されているのと等価である。

【００５１】

２０１は多重化を解く分解器であり、オーディオ符号化データとビデオ符号化データを分離する。ビデオ符号化データはパケット化された単位ごとに後段に出力される。

【００５２】

２０２は出力端子であり、外部のオーディオ復号器にオーディオ符号化データを出力する。２０３は入力されたビデオ符号化データからVOPスタートコードの位置にある符号化データβを抽出するスタートコード検出器である。２０４はスタートコードの位置に該当する符号化データ以外の符号化データを格納しておくバッファである。２０５は符号化データβから正しいVOPスタートコードではない場合、VOPスタートコードとの差異を抽出するエラー解析器である。２０６は暗号を所定の方式で解読する暗号解読器である。２０７は認証器であり、符号化データから抽出された認証データと入力された認証データを比較し、同じであった場合にセキュリティの解除を決定する。２０８は本画像データ処理装置に固有な認証データを格納した認証メモリである。

【００５３】

２０９、２１１はセレクタであり、認証器２０７とエラー解析器２０５の指示に従ってそれぞれの入出力を選択する。２１０はスクランブルを解除するデスクランブラである。２１２はビデオ符号化データを復号するビデオ復号器である。２１３は復号されて再生された画像データを出力する出力端子である。

【００５４】

上述のように構成された画像データ処理装置の動作を以下に説明する。

【００５５】

入力端子２００から入力された符号化データは分離器２０１に入力される。分離器２０１はパケット単位の符号化データをビデオ符号化データとオーディオ符号化データとに分離し、オーディオ符号化データを出力端子２０２から外部に出

力する。

【００５６】

ビデオ符号化データはスタートコード検出器２０３に入力される。スタートコードであるVOPスタートコードは、フレーム単位で符号化されパケット化されたとき必ず先頭の３２ビットに位置している。そのため、先頭から３２ビットの符号化データを抽出してエラー解析器２０５に出力し、残りをバッファ２０４に出力する。

【００５７】

エラー解析器２０５は入力された３２ビットの符号化データとVOPスタートコードを比較し、その差異を求める。すなわち、入力データとVOPスタートコードの値（000001B6）と論理的排他和を求め、右に９ビットシフトする。その結果は暗号解読器２０６に入力される。

【００５８】

また、VOPスタートコードとまったく同じ、すなわちセキュリティが施されていない場合はセレクタ２０９、２１１にそれぞれを直結して入力された符号化データがそのままビデオ復号器２１２に入力されるように指示する。

【００５９】

また、セキュリティが施されている場合でセレクタ２０９、２１１に認証器２０７の出力が正しく認証されたことを示している場合はデスクランブラ２１０を経由するように入出力先を制御し、正しく認証できなかった場合にはセレクタ２０９、２１１にそれぞれを直結して入力された符号化データがそのままビデオ復号器２１２に入力されるように指示する。

【００６０】

暗号解読器２０６は所定の方式で暗号を解読し、スクランブルのキーと認証データを獲得する。この解読方式は第１実施例の暗号化器１０９の暗号を解読する方式を示す。暗号解読によって得られたキーはデスクランブラ２１０に入力され、認証データは認証器２０７に入力される。

【００６１】

認証メモリ２０８は本装置に固有な認証データが格納されている。認証器２０

７は暗号解読器２０６から入力された認証データと認証メモリ２０８の認証データを比較し、正しく認証できた場合でエラー解析器２０５で暗号化データの存在が検知できたときにはセレクタ２０９、２１１はデスクランブラ２１０での処理を選択させ、そうでなければ直結を指示する。

【００６２】

セレクタ２１１からの出力はビデオ復号器２１２に入力される。ビデオ復号器２１２は入力データを復号し、再生画像を生成する。この結果、ビデオ復号器２１２はセキュリティが施されていないフレームに関してはバッファ２０４、セレクタ２０９、２１１を介して分離器２０１からの出力をそのまま入力して復号することで通常の再生画像を得ることができる。

【００６３】

また、セキュリティがかかっていた場合、正しく認証ができなければスクランブルされたビデオ符号化データが入力され、スタートコードに暗号データが重畳されているままなのでスタートコードを検出できず、復号ができないため再生画像を得ることはできない。セキュリティがかかっていても正しく認証できればスクランブルが解除され正しい再生画像を得ることが可能になる。

【００６４】

このような一連の選択、暗号解読、復号化処理によりセキュリティに対応した画像の再生を実施できる。

【００６５】

尚、本実施例ではエラー解析器２０５の出力を暗号解読器２０６に入力したが、これに加えてエラーの有無を検証し、エラーがあればビデオ復号器２１２の動作を停止させるように制御することも可能である。これにより、先頭にスタートコードを検出する機能がなく、誤ったデータでビデオ復号器２１２が誤動作することを防ぐことができる。

【００６６】

＜第３実施例＞

図３は、本発明の第３の実施例としての画像データ処理装置の構成を示すブロック図である。尚、上述の第１実施例（図１）と同様の構成要素については同一

番号を付してその詳細な説明は省略する。

【００６７】

３０１は操作者が認証データを設定する認証設定器である。３０２はIPMP符号化データを生成するIPMP符号化器である。３０３は暗号化器であり、第1実施例の暗号化器１０９と同様に暗号化を行うが、キーのみを暗号化する。３０４は第1実施例の暗号重畳器１０６と同様に暗号化データをスタートコードに重畳する。３０５は多重化器であり、第1実施例の多重化器１１４の画像データ符号化データとオーディオ符号化データの入力に加え、IPMP符号化データも多重化する。

【００６８】

上述のように構成された画像データ処理の動作を以下で説明する。

【００６９】

まず、操作者は、第１実施例と同様にセキュリティ設定器１０４で著作権を保護するデータの区間を決定し、設定する。認証設定器３０１は認証に必要なデータたとえばパスワードを操作者が設定し、IPMP符号化器３０２に入力する。IPMP符号化器３０２はIPMPの書式にしたがってビデオ符号化データに対してセキュリティを施すことと認証設定器３０１で設定された認証に必要なデータを暗号化、符号化する。IPMP符号化器３０２の出力はビデオ符号化データ、オーディオ符号化データに先駆けて多重化器３０５で多重化されて出力端子１１５から出力される。

【００７０】

入力端子１００からフレーム単位で画像データが入力され、ビデオ符号化器１０１で符号化され、フレーム単位でセレクタ１０２に入力される。セキュリティ設定器１０４でセキュリティを施さないフレームとしていた場合、第１実施例と同様に符号化データにはスクランブル等のセキュリティは施されず、出力端子１１５から出力される。

【００７１】

次に、セキュリティ設定器１０４でセキュリティを施すフレームとしていた場合について述べる。

【００７２】

セキュリティ設定器１０４はキー生成器１０８に該当するフレームのスクランブルのときに使用するキーを生成させる。生成されたキーはスクランブラ１０７と暗号化器３０３に入力される。また、暗号化器３０３は前記キーを所定の暗号化方式で暗号化し、３２ビット以下の暗号データを生成する。本実施例では３２ビットの暗号データγを生成するものとする。

【００７３】

セレクタ１０２は出力先をスタートコード検出器１０５とし、セレクタ１１２は入力先を合成器１１１とする。従って、セレクタ１０２に入力された符号化データはスタートコード検出器１０５に入力される。スタートコード検出器１０５はVOPスタートコードを検出する。それ以外の符号化データはスクランブラ１０７に入力される。検出されたVOPスタートコードは暗号重畳器３０４ に入力される。暗号重畳器３０４では暗号データγをVOPスタートコードと論理的排他和をとる。例えば暗号データγが１６進で“7234A19C”であったとき暗号重畳器３０４の出力は“7234A02A”となる。

【００７４】

キー生成器１０８で生成されたキーはスクランブラ１０７に入力され、このキーを使ってスタートコードを除く符号化データに対してスクランブルを施し、合成器１１１に入力される。合成器１１１はVOPスタートコードに暗号データγを重畳した結果を先頭に、スクランブルが施された符号化データと合成する。

【００７５】

出力端子１１５からは外部で符号化されたオーディオ符号化データが入力され、多重化器３０５でフレーム単位でセレクタから出力されるビデオ符号化データと多重化してパケット化して出力端子１１５から出力される。

【００７６】

上述のような一連の符号化、暗号化、選択処理によりセキュリティを施した符号化データを、冗長を生じることなく実施できる。ビデオのセキュリティの詳細はビデオの符号化データ内に内包し、全体をIPMPで管理することにより、ビデオデータの管理を容易にすることもできる。

【００７７】

＜第４実施例＞

図４は、本発明の第４の実施例としての画像データ処理装置の構成を示すブロック図である。尚、上述の第２実施例（図２）と同様の構成要素については同一番号を付してその詳細な説明は省略する。また、本実施例では第３実施例で生成された符号化データを処理するものとし、図４の入力端子２００は図３の出力端子１１５に接続されているのと等価である。

【００７８】

図４において、４０１ は多重化を解く分離器であり、IPMP符号化データ、オーディオ符号化データ、ビデオ符号化データを分離する。ビデオ符号化データはパケット化された単位ごとに後段に出力される。４０２はIPMP復号器であり、IPMP情報を復号する。

【００７９】

４０３は操作者が認証データを入力するための端末である。４０４はスタートコード検出器２０３で抽出された符号化データとVOPスタートコードとの差異を抽出するエラー解析器である。４０５は暗号を所定の方式で解読する暗号解読器である。４０６はビデオ復号器であり、再生画像のデータと正しく復号できたか否かを出力する。４０７はフレームメモリであり、最後に正しく復号された画像データを１フレーム分保持する。４０８はセレクタであり、ビデオ復号器４０６の復号結果にしたがってビデオ復号器４０６からの出力かフレームメモリ４０７からの出力かを選択して出力する。

【００８０】

上述のように構成された画像データ処理装置の動作を以下で説明する。

【００８１】

入力端子２００から入力された符号化データは分離器４０１に入力される。分離器４０１はIPMP符号化データとパケット単位の符号化データをビデオ符号化データとオーディオ符号化データとに分離する。そのうち、オーディオ符号化データを出力端子２０２から外部に出力する。

【００８２】

IPMP符号化データはIPMP復号器４０２に出力される。IPMP復号器４０２はIPMP

符号化データを復号し、IPMPに関する情報、この場合はシーケンスに関する認証データを復号して獲得する。認証データは認証器２０７に入力され端末４０３からの操作者による認証データの入力を促す。

【００８３】

また、分離器４０１で分離されたビデオ符号化データはスタートコード検出器２０３に入力され、第２実施例と同様にスタートコードに該当する符号化データとそれ以外を分離し、スタートコードに該当するデータをエラー解析器４０４に、それ以外をバッファ２０４に出力する。

【００８４】

認証器２０７は端末４０３から入力された認証データとIPMP復号器４０２から入力された認証データを比較し、正しく認証できた場合でエラー解析器４０４で暗号化データの存在が検知できたときにはセレクタ２０９、２１１はデスクランブラ２１０での処理を選択させ、そうでなければ直結を指示する。

【００８５】

エラー解析器４０４は入力された３２ビットの符号化データとVOPスタートコードを比較し、その差異を求める。すなわち、入力データとVOPスタートコードの値（000001B6）と論理的排他和を求める。その結果は暗号解読器４０５に入力される。

【００８６】

また、セキュリティが施されていない場合はセレクタ２０９、２１１にそれぞれを直結して入力された符号化データがそのままビデオ復号器４０６に入力されるように指示する。

【００８７】

また、セキュリティが施されている場合でセレクタ２０９、２１１に認証器２０７の出力が正しく認証されたことを示している場合はデスクランブラ２１０を経由するように入出力先を制御し、正しく認証できなかった場合にはセレクタ２０９、２１１にそれぞれを直結して入力された符号化データがそのままビデオ復号器４０６に入力されるように指示する。

【００８８】

暗号解読器４０５は所定の方式で暗号を解読し、スクランブルのキーを獲得する。暗号解読によって得られたキーはデスクランブラ２１０に入力される。

【００８９】

セレクタ２１１からの出力はビデオ復号器４０６に入力される。ビデオ復号器４０６は入力データを復号し、再生画像を生成する。この結果、ビデオ復号器４０６はセキュリティが施されていないフレームに関してはバッファ２０４、セレクタ２０９、２１１を介して分離器４０１からの出力をそのまま入力して復号することで通常の再生画像を得ることができる。このデータはセレクタ４０８を介して出力端子２１３から外部に出力され、同時にフレームメモリ４０７に格納される。

【００９０】

また、セキュリティが施されていた場合、正しく認証ができなければスクランブルされたビデオ符号化データが入力され、スタートコードに暗号データが重畳されているままなのでスタートコードを検出できず、復号ができない。この場合、セレクタ４０８は正しく復号された最後のフレームデータをフレームメモリ４０７から読み出し、端子２１３に出力する。この時、フレームメモリ４０７の内容は更新されない。

【００９１】

セキュリティがかかっていても正しく認証できればスクランブルが解除され正しい再生画像を得ることが可能になる。この場合もセレクタ４０８を介して出力端子２１３から外部に出力され、同時にフレームメモリ４０７に格納される。

【００９２】

このような一連の選択、暗号解読、復号化処理によりセキュリティに対応した画像の再生を実施できる。画像のスクランブルに関する情報をビデオの符号化データに重畳してあるのでフレーム単位での管理も容易になる。さらに、復号ができない場合でも正しく再生された画像を出すことで、いきなり画像が表示されなくなったり、ノイズ画面が出たりしなくなったので、操作者に不快感を与えないようにすることができる。

【００９３】

＜第５実施例＞

図５ は、本発明の第５の実施例としての画像データ処理装置の構成を示すブロック図である。尚、本実施例では特に画像データの符号化処理について説明する。また、本実施例ではMPEG-1符号化方式を例にとって説明するが、特にこれに限定されることではない。MPEG-1の詳細な仕様についてはISO 11172－2を参照されたい。

【００９４】

図５において、５００は装置全体の制御、及び種々の処理を行う中央演算装置（CPU）、５０１は本装置の制御に必要なオペレーティングシステム（OS）、ソフトウェア、演算に必要な必要な記憶領域を提供するメモリである。尚、メモリ５０１には装置全体を制御し、各種ソフトウェアを動作させるためのOSや動作させるソフトウェアを格納し、画像データを符号化のために読み込む画像エリア、一時的に符号データを格納する符号エリア、各種演算のパラメータ等を格納しておくワーキングエリアが存在する。

【００９５】

５０２は種々の装置をつなぎ、データ、制御信号をやり取りするバス、５０３はソフトウェアを蓄積する記憶装置、５０４は動画像データを蓄積する記憶装置、５０５は画像を表示するモニタであり、５０８は通信回路であり、LAN、公衆回線、無線回線、放送電波等で構成されている。５０７は通信回路５０８に符号化データを送信する通信インターフェースである。５０６は装置を起動したり、セキュリティを設定したりするための端末である。

【００９６】

上述のように構成においてまず、処理に先立ち、端末５０６から記憶装置５０４に蓄積されている動画像データから符号化する動画像データを選択し、装置の起動が指示される。すると記憶装置５０３に格納されているソフトウェアがバス５０２を介してメモリ５０１に展開され、ソフトウェアが起動される。

【００９７】

以下、CPU５００による記憶装置５０４に格納されている動画像データの符号化動作を図６、図７に示すフローチャートに従って説明する。

【００９８】

まず、図６を用いて符号化処理を説明する。

【００９９】

図６において、ステップＳ１ではシーケンス単位で認証を行う「シーケンス認証データ」、シーンの集合単位で認証を行う「シーン認証データ」、セキュリティを施して復号の禁止を開始するピクチャ、禁止を解除するピクチャ、ピクチャ単位での認証を行う「ピクチャ認証データ」などのセキュリティの設定条件を入力し、これらをメモリ５０１のワーキングエリアに格納し、ステップＳ２に進む。

【０１００】

ステップＳ２では「シーケンス認証データ」を暗号化し、MPEG-1符号化方式のシーケンスヘッダコード（値“000001B3”）に排他的論理和によって重畳し、メモリ５０１の所定の領域に格納し、ステップＳ３に進む。

【０１０１】

ステップＳ３では他のシーケンスレイヤの符号化データを生成し、重畳されたシーケンスヘッダコードに続けて格納し、パケットとして記憶装置５０４の所定の領域に蓄積し、ステップＳ４に進む。

【０１０２】

ステップＳ４ではGOPを１つのシーンとして考えたとき、符号化対象の全シーンの画像データについて処理を終了したか否かを判定する。もし全ての画像データの処理が終了していればソフトウェアを終了する。そうでなければ、ステップＳ５に進む。

【０１０３】

ステップＳ５では「GOP認証データ」を暗号化し、MPEG-1符号化方式のGOPスタートコード（値“000001B7”）に排他的論理和によって重畳し、メモリ５０１の所定の領域に格納し、ステップＳ６に進む。

【０１０４】

ステップＳ６では他のGOPレイヤの符号化データを生成し、重畳されたGOPスタートコードに続けて格納し、パケットとして記憶装置５０４の所定の領域に蓄積

し、ステップＳ７に進む。

【０１０５】

ステップＳ７ではGOP内の符号化対象の全ピクチャ画像データについて符号化処理を終了したか否かを判定する。もし全ての画像データの符号化処理が終了していればGOPの符号化処理を終了し、次のGOPの符号化処理をするため、ステップＳ４に進む。そうでなければ、ステップＳ８に進み、各ピクチャ単位の符号化を行う。

【０１０６】

次に、図６のステップＳ８の各ピクチャ単位での符号化処理を図７を用いて説明する。

【０１０７】

図７において、ステップＳ１０では、図６のステップＳ１で設定してメモリ５０１上のワーキングエリアに格納されたピクチャの条件にしたがって、符号化対象のピクチャ画像データがセキュリティを施す必要があるか否かを判定する。もし符号化するピクチャがセキュリティを施す区間に含まれていれば暗号化処理を行うため、ステップＳ１２に進む。そうでなければ、ステップＳ１１に進み、通常どおりのピクチャの符号化を行う。

【０１０８】

ステップＳ１１では記憶装置５０４から符号化するピクチャの画像データを読み出し、MPEG-1符号化方式のピクチャレイヤの符号化を行い、パケットとして記憶装置５０４の所定の領域に蓄積し、次のピクチャの処理をするため、図６のステップＳ７に進む。

【０１０９】

ステップＳ１２ではスクランブルのためのキーを生成し、生成したキーと「ピクチャ認証データ」を暗号化し、MPEG-1符号化方式のピクチャスタートコード（値“00000100”）に排他的論理和によって重畳し、メモリ５０１の所定の領域に格納し、ステップＳ１３に進む。

【０１１０】

ステップＳ１３では他のピクチャレイヤのヘッダに関する符号化データを生成

し、重畳されたピクチャスタートコードに続けて格納する。さらに記憶装置５０４から符号化するピクチャの画像データを読み出し、符号化してメモリ５０１の符号エリアに一時的に格納する。

【０１１１】

ステップＳ１４ではステップＳ１３で生成した符号化データに対して、ステップＳ１２で生成したキーを使ってスクランブル処理を行いステップＳ１５に進む。

【０１１２】

ステップＳ１５では重畳されたピクチャスタートコードとスクランブルされた符号化データをパケットとして記憶装置５０４の所定の領域に蓄積し、ステップＳ７に進む。

【０１１３】

上述のような一連の符号化、暗号化、選択処理によりセキュリティを施した符号化データを、冗長データを発生することなく実施できる。各レイヤでセキュリティを行うことができるのでさまざまなレベルのセキュリティに対応することもできる。

【０１１４】

尚、上述の実施例では記憶装置５０４に蓄積する例を述べたが、通信インターフェース５０５を介して通信回線５０６に送出してもよい。

【０１１５】

＜第６実施例＞

本実施例では特に画像データの復号化処理について説明する。画像データ処理装置の構成は第５実施例の図５と同様である。尚、本実施例においてもMPEG-1符号化方式を例にとって説明するが、特にこれに限定されることではない。また、本実施例では第５実施例で生成され、記憶装置５０４に格納された符号化データの復号処理を例にとって説明する。

【０１１６】

図５の構成において、処理に先立ち、端末５０６から記憶装置５０４に蓄積されている動画像符号化データから復号する符号化データを選択し、装置の起動が

指示されると記憶装置５０３に格納されているソフトウェアがバス５０２を介してメモリ５０１に展開され、ソフトウェアが起動される。

【０１１７】

以下、CPU５００による記憶装置５０４に格納されている符号化データの復号動作を図８、図９に示すフローチャートに従って説明する。

【０１１８】

まず、図８を用いて復号化処理を説明する。

【０１１９】

図８において、ステップＳ２０では記憶装置５０４から復号するシーケンスの最初のパケットを読み出し、メモリ５０１の符号エリアに格納する。格納された符号化データから先頭の３２ビットをシーケンスヘッダコードと比較し、重畳された「シーケンス認証データ」を分離し、暗号を解読し、ステップＳ２１に進む。

【０１２０】

ステップＳ２１では解読された「シーケンス認証データ」と端末５０６から入力された認証データと比較し、正しく認証された場合ステップＳ２２に進み、復号処理を継続する。正しく認証されない場合は復号処理を終了し、ソフトウェアを終了する。

【０１２１】

ステップＳ２２ではメモリ５０１の符号エリアに格納された他のシーケンスレイヤの符号化データを復号し、後段の処理で使用できるように、その結果をメモリ５０１のワーキングエリアに格納し、ステップＳ２３に進む。

【０１２２】

ステップＳ２３では全シーン(GOP)の画像データについて処理を終了したか否かを判定する。もし全ての画像データの処理が終了していればソフトウェアを終了する。そうでなければ、ステップＳ２４に進む。

【０１２３】

ステップＳ２４では記憶装置５０４から復号するGOPのヘッダに関するパケットを読み出し、メモリ５０１の符号エリアに格納する。格納された符号化データ

から先頭の３２ビットをGOPスタートコードと比較し、重畳された「GOP認証データ」を分離し、暗号を解読し、ステップＳ２５に進む。

【０１２４】

ステップＳ２５では解読された「GOP認証データ」と端末５０６から入力された認証データと比較し、正しく認証された場合はステップＳ２６に進み、復号処理を継続する。正しく認証されない場合はステップＳ２３に進み、次のGOPの処理を試みる。

【０１２５】

ステップＳ２６ではメモリ５０１の符号エリアに格納された他のGOPレイヤの符号化データを復号し、後段の処理で使用できるように、その結果をメモリ５０１のワーキングエリアに格納し、ステップＳ２７に進む。

【０１２６】

ステップＳ２７ではGOP内の復号対象の全ピクチャ画像データについて処理を終了したか否かを判定する。もし全ての画像データの復号処理が終了していればGOPの復号処理を終了し、次のGOPの復号処理をするため、ステップＳ２３に進む。そうでなければ、ステップＳ２８に進み、各ピクチャ単位の復号を行う。

【０１２７】

次に、図８のステップＳ２８の各ピクチャ単位での復号化処理を図９を用いて説明する。

【０１２８】

図９において、ステップＳ３１では記憶装置５０４から復号するピクチャに関するパケットを読み出し、メモリ５０１の符号エリアに格納する。

【０１２９】

ステップＳ３２ではメモリ５０１に格納された符号化データから先頭の３２ビットをピクチャスタートコードと比較し、値が“00000100”であればステップＳ３３に進み、通常どおりのピクチャの復号を行う。すなわちセキュリティは施されていない。また値が“00000100”でなければセキュリティが施されているとし、ステップＳ３４に進み、処理を行う。

【０１３０】

ステップＳ３３ではメモリ５０１の符号エリアから復号するピクチャの符号化データを読み出し、MPEG-1符号化方式のピクチャレイヤの復号を行い、モニタ５０５に送られ、表示される。さらに次のピクチャの処理をするため、図８のステップＳ２７に進む。

【０１３１】

一方、ステップＳ３４では重畳された「ピクチャ認証データ」とスクランブルのキーを分離し、暗号を解読し、ステップＳ３５に進む。

【０１３２】

ステップＳ３５では解読された「ピクチャ認証データ」と端末５０６から入力された認証データと比較し、正しく認証された場合ステップＳ３６に進み、復号処理を継続する。正しく認証されない場合は次のピクチャの処理をするため、図８のステップＳ２７に進む。

【０１３３】

ステップＳ３６ではメモリ５０１の符号エリアに格納されたピクチャレイヤの符号化データを読み出しスクランブルを暗号解読によって得られたキーでデスクランブルし、ステップＳ３７に進む。

【０１３４】

ステップＳ３７ではデスクランブルされたピクチャの符号化データをMPEG-1符号化方式のピクチャレイヤの復号を行い、モニタ５０５に送り、表示する。さらに次のピクチャの処理をするため、図８のステップＳ２７に進む。

【０１３５】

このような一連の選択、暗号解読、復号化処理によりセキュリティに対応した画像の再生を実施できる。

【０１３６】

各レイヤでセキュリティを行うことができるのでさまざまなレベルのセキュリティに対応でき、それぞれの認証データの解読ができないシステムでは各スタートコードを認識できないため、まったく再生を行うことはできず、著作権を保護することができる。

【０１３７】

【発明の効果】

以上の説明から明らかなように、本発明では、冗長データの付加を抑えながらセキュリティを施した符号化データを生成することできる。

【０１３８】

また、本発明ではセキュリティデータを階層に応じて設定することも可能となる。ピクチャやフレーム単位で管理が行えるので編集等にも好適に扱うことができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施例としての画像データ処理装置の構成を示すブロック図である。

【図２】

本発明の第２の実施例としての画像データ処理装置の構成を示すブロック図である。

【図３】

本発明の第３の実施例としての画像データ処理装置の構成を示すブロック図である。

【図４】

本発明の第４の実施例としての画像データ処理装置の構成を示すブロック図である。

【図５】

本発明の第５及び第６の実施例としての画像データ処理装置の構成を示すブロック図である。

【図６】

本発明の第５実施例における画像の符号化の工程を現すフローチャート図である。

【図７】

本発明の第５実施例における画像の符号化の工程を現すフローチャート図である。

【図８】

本発明の第６実施例における画像の復号の工程を現すフローチャート図である。

【図９】

本発明の第６実施例における画像の復号の工程を現すフローチャート図である。

【図１０】

従来例を示すブロック図である。

【図１１】

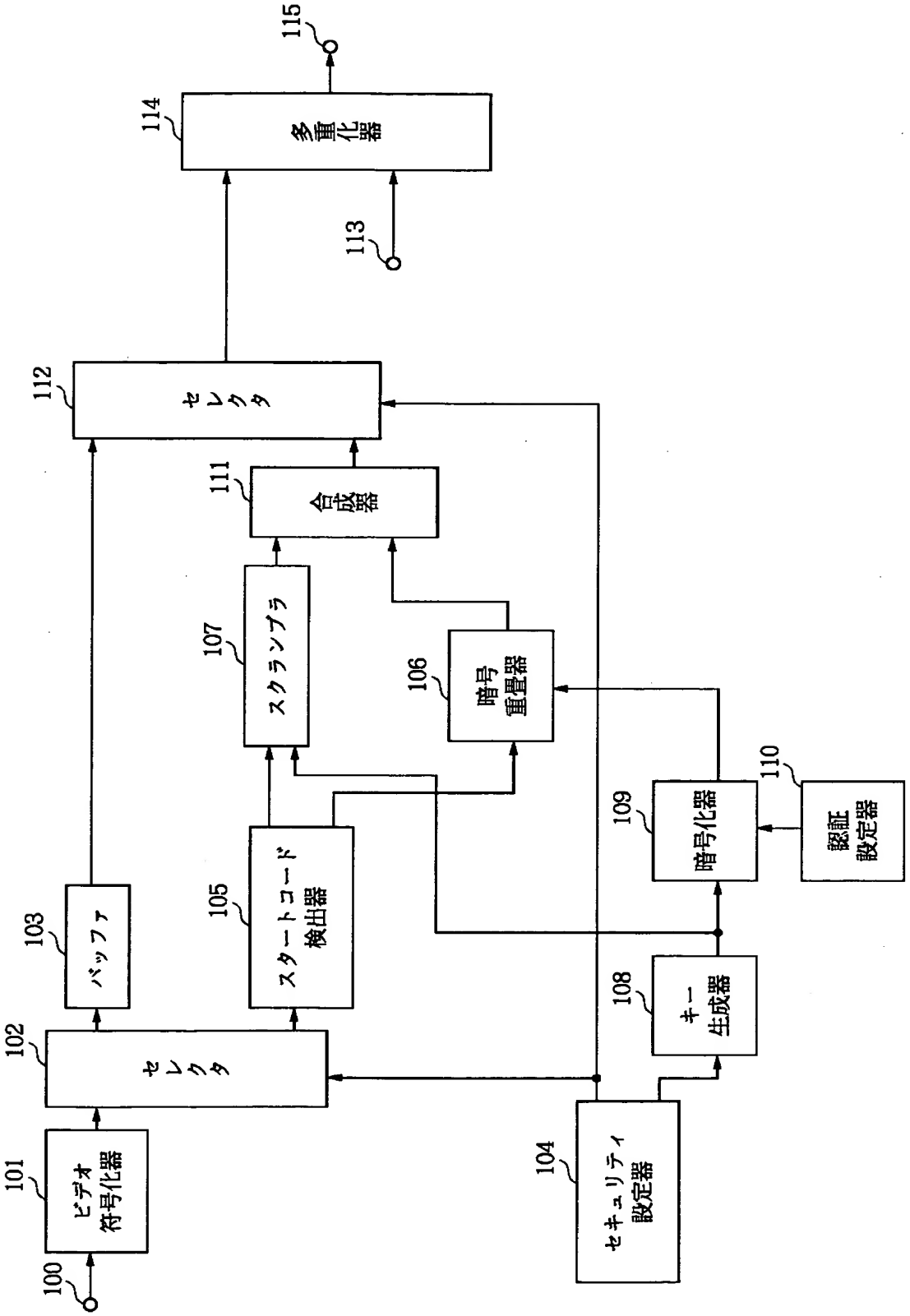
MPEG-4のビットストリームの構成例を示す図である。

【図１２】

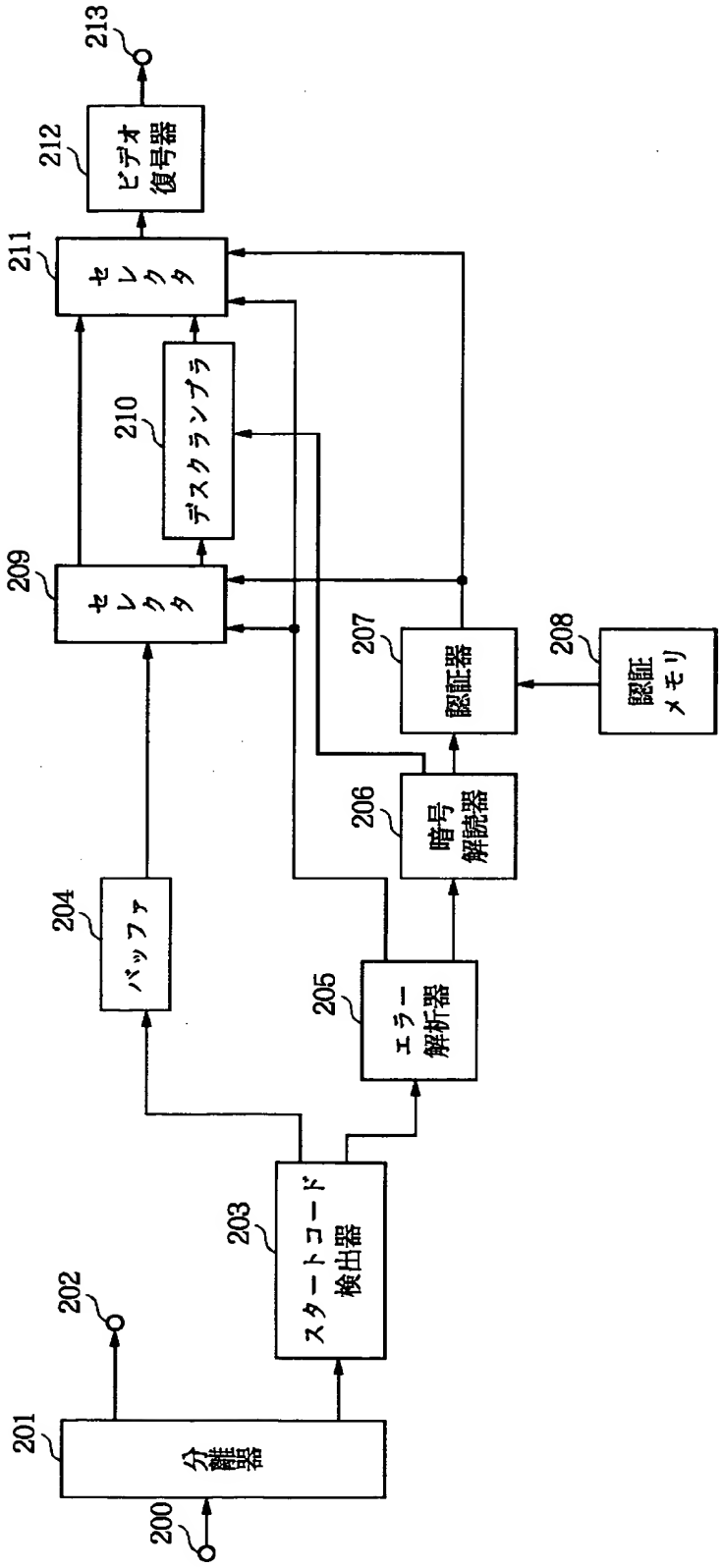
IPMP符号化データに含まれる情報の例を示す図である。

【書類名】　　図面

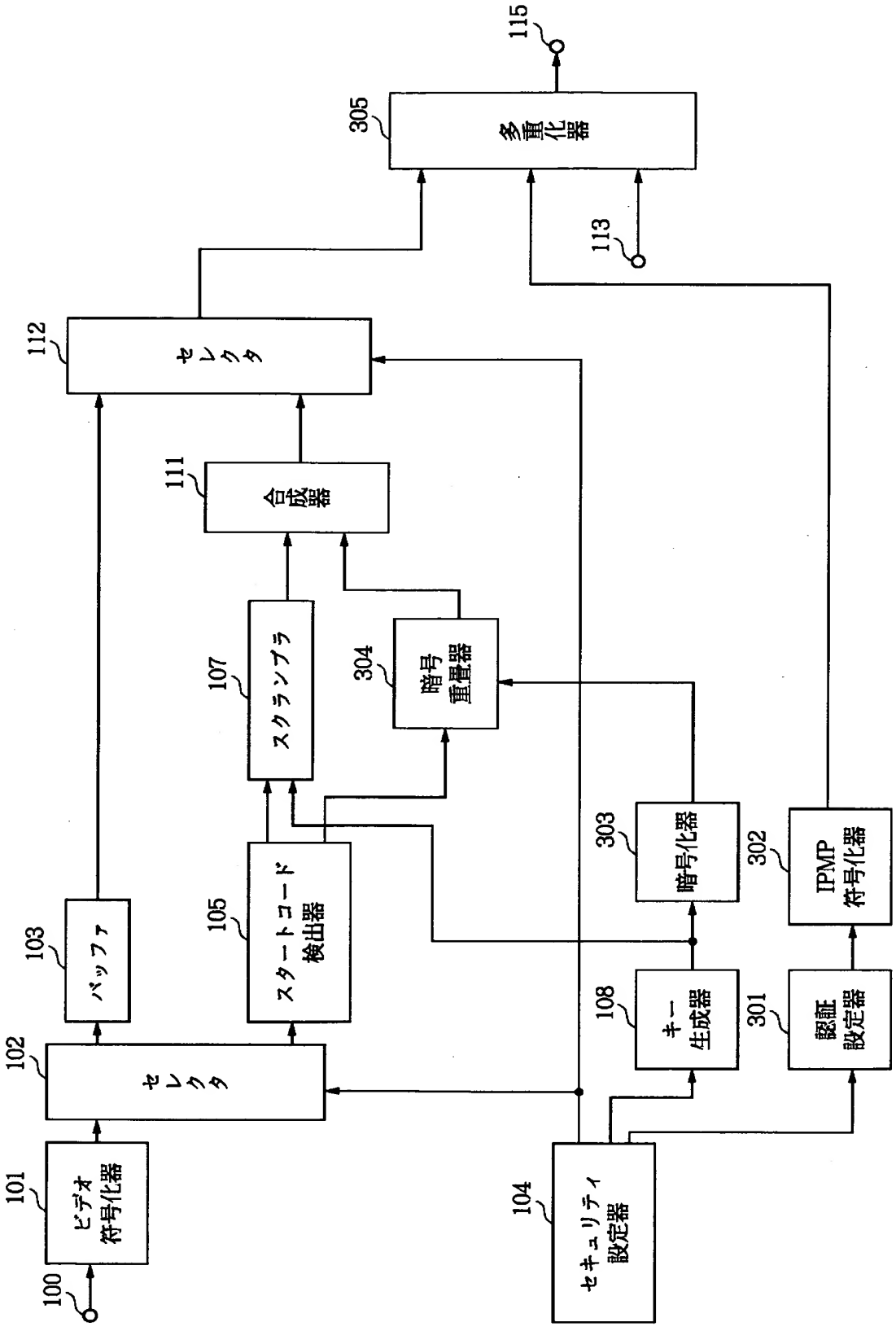
【図１】


100
ビデオ符号化器
101
セレクタ
102
バッファ
103
セキュリティ設定器
104
スタートコード検出器
105
暗号重畳器
106
スクランブラ
107
キー生成器
108
暗号化器
109
認証設定器
110
合成器
111
セレクタ
112
113
多重化器
114
115

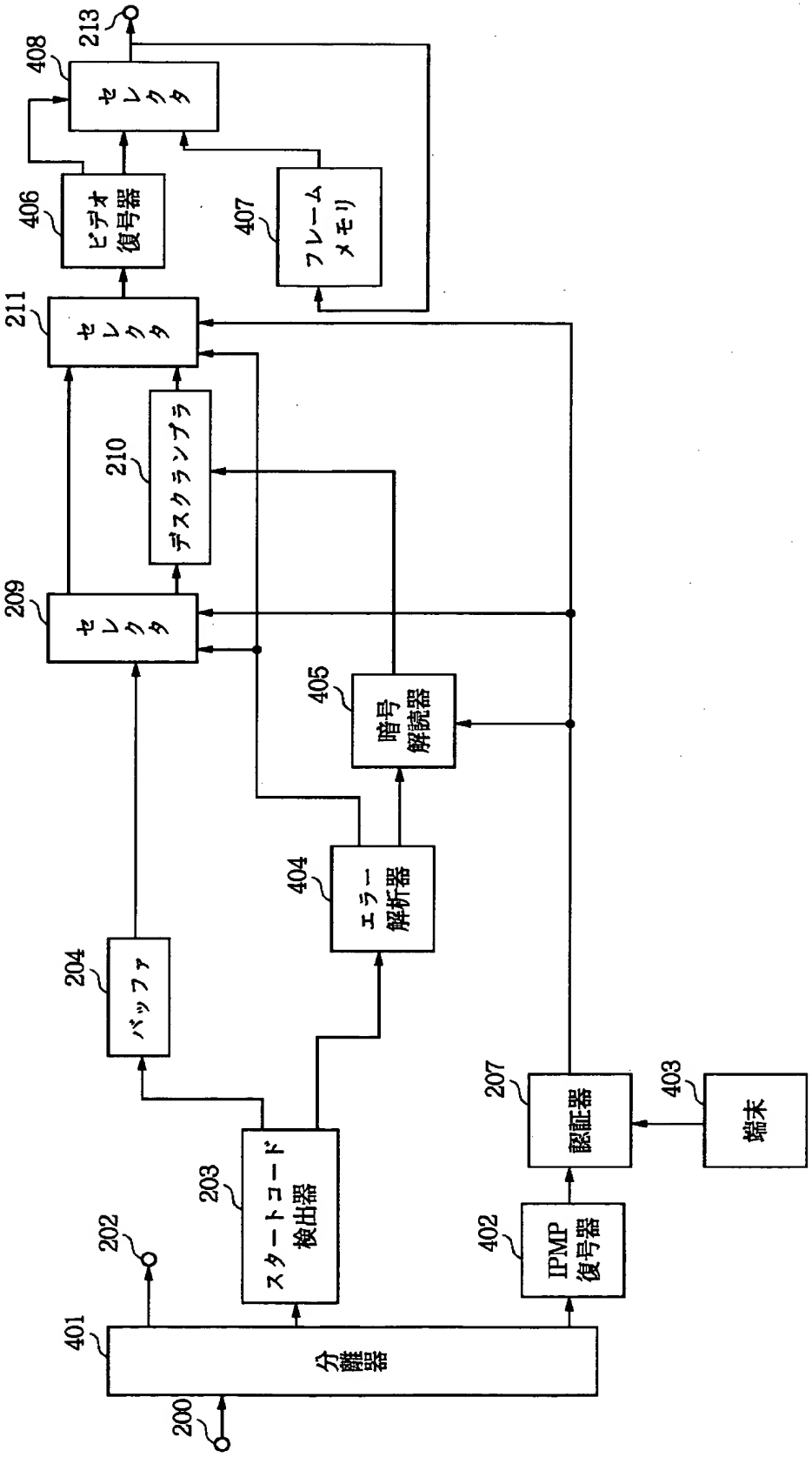
【図２】


213
212
ビデオ復号器
211
セレクタ
210
デスクランブラ
209
セレクタ
207
認証器
208
認証メモリ
206
暗号解読器
204
バッファ
205
エラー解析器
203
スタートコード検出器
202
201
分離器
200

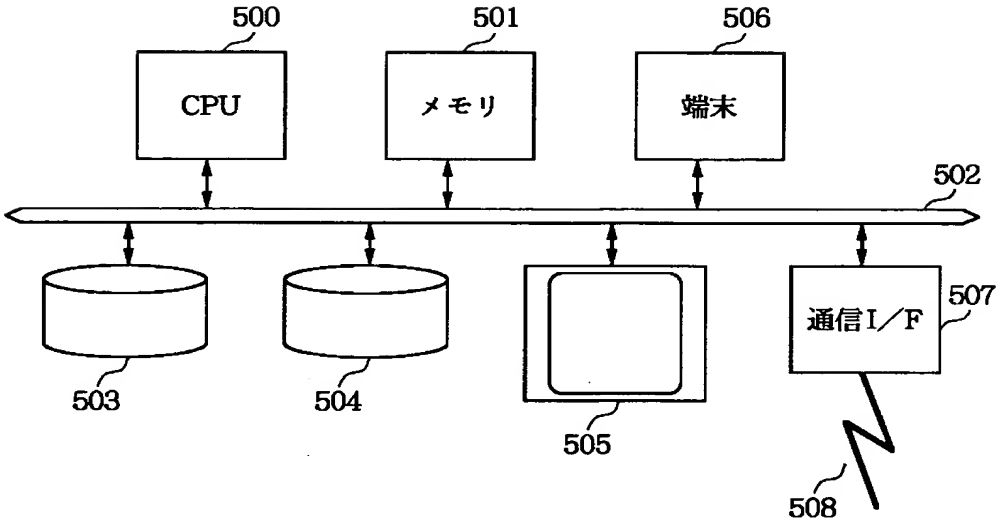
【図３】


100
101
ビデオ符号化器
102
セレクタ
103
バッファ
104
セキュリティ設定器
105
スタートコード検出器
107
スクランブラ
108
キー生成器
111
合成器
112
セレクタ
113
115
301
認証設定器
302
IPMP符号化器
303
暗号化器
304
暗号重畳器
305
多重化器

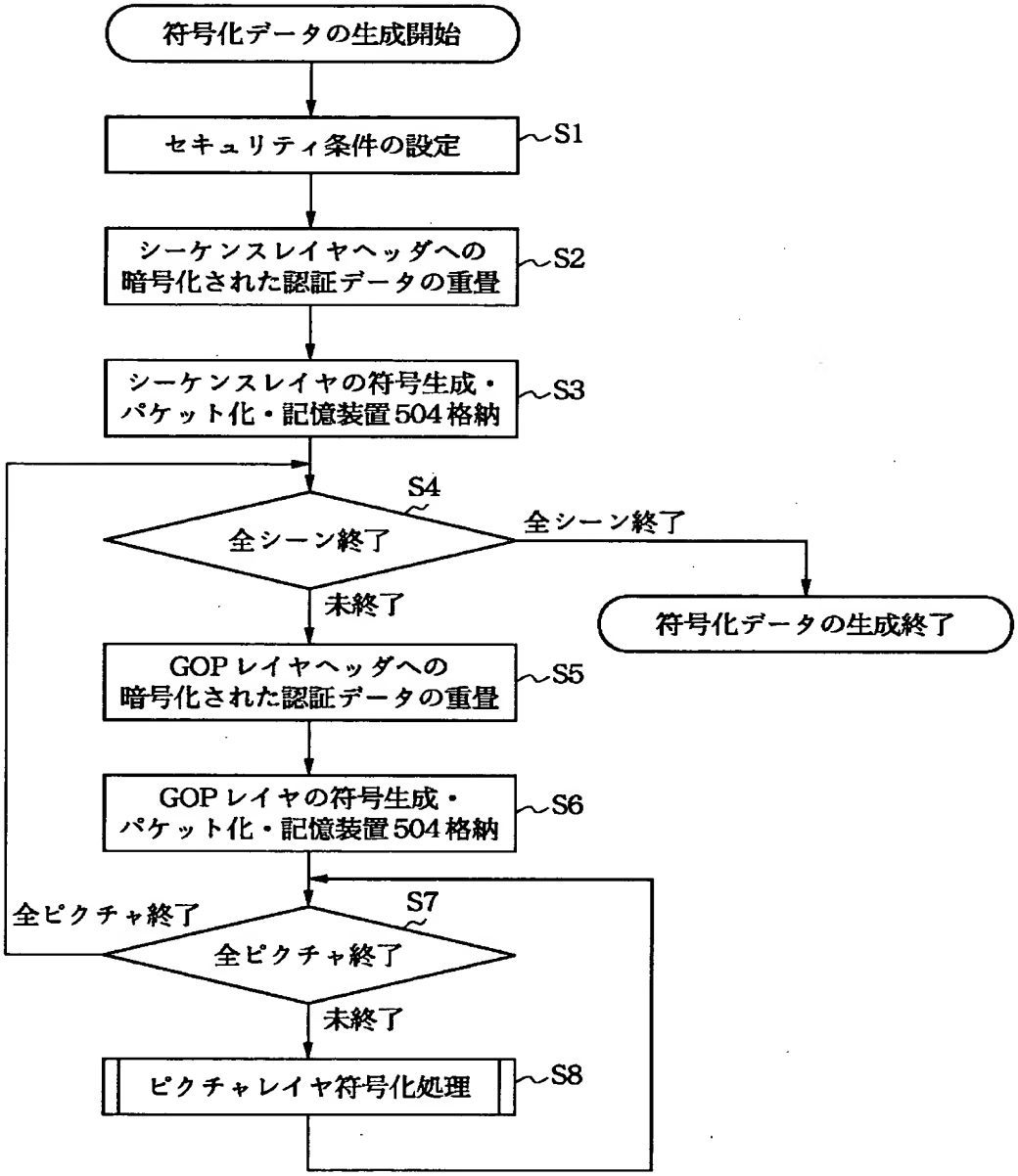
【図４】


213
408
セレクタ
406
ビデオ復号器
407
フレームメモリ
211
セレクタ
210
デスクランブラ
209
セレクタ
405
暗号解読器
404
エラー解析器
204
バッファ
207
認証器
403
端末
203
スタートコード検出器
202
402
IPMP復号器
401
分離器
200

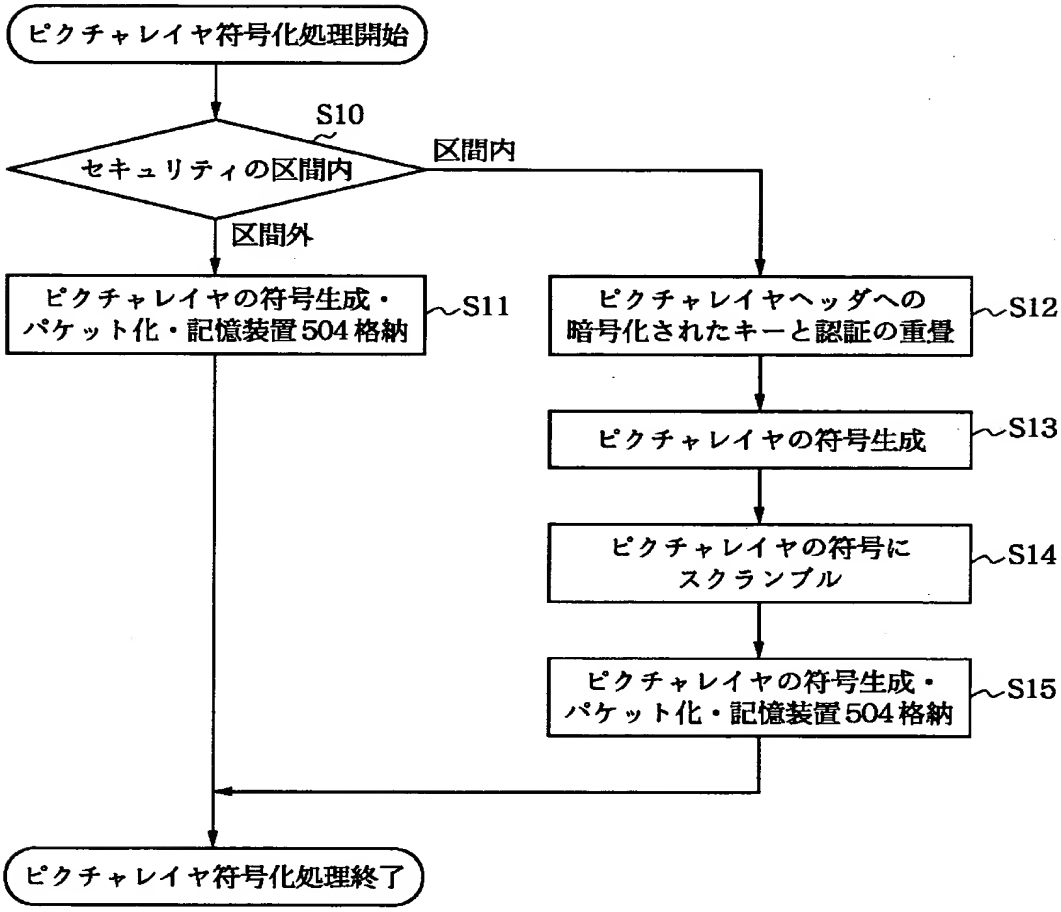
【図５】



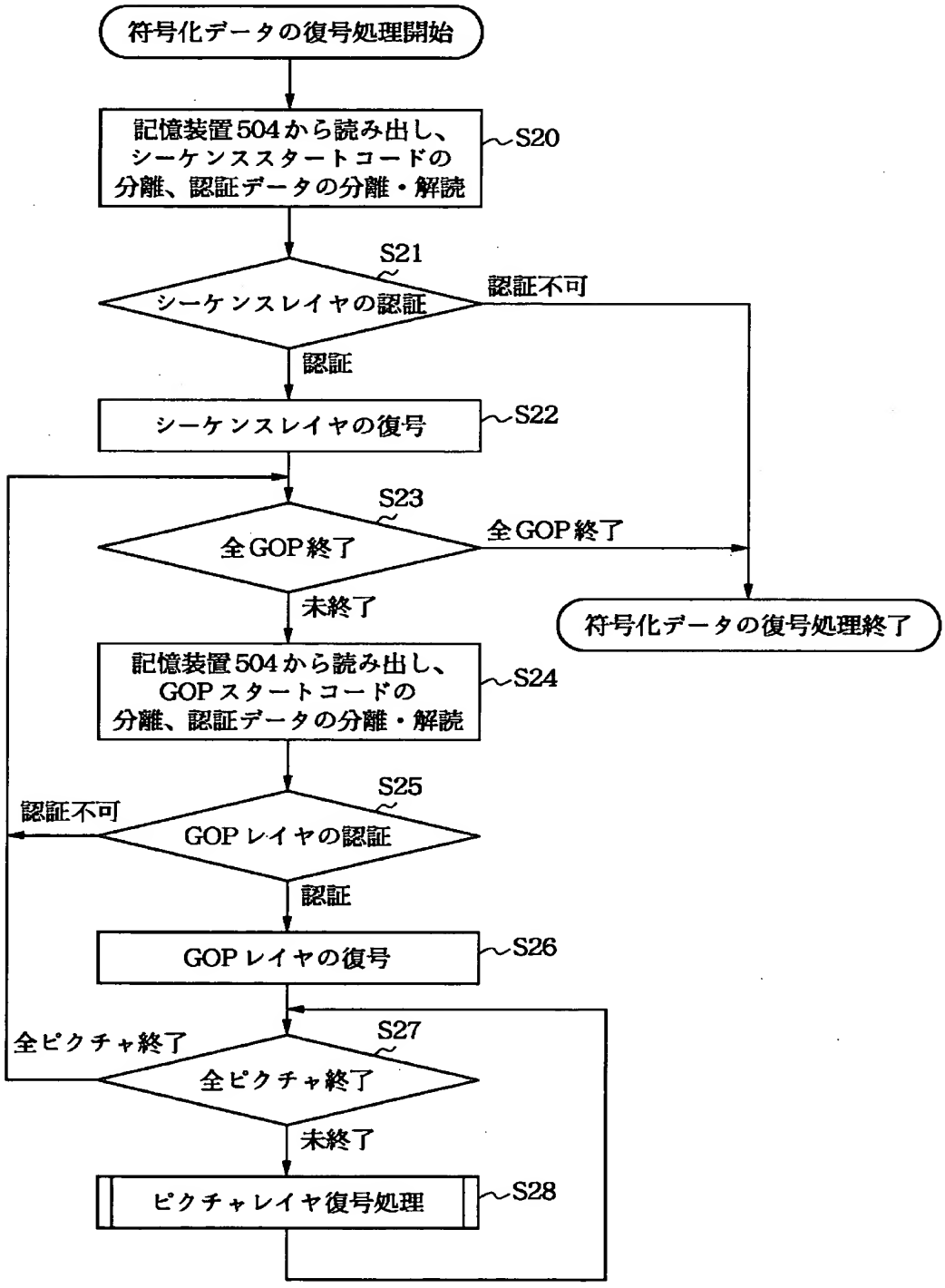
【図６】


符号化データの生成開始
セキュリティ条件の設定
S1
シーケンスレイヤヘッダへの
暗号化された認証データの重畳
S2
シーケンスレイヤの符号生成・
パケット化・記憶装置504格納
S3
S4
全シーン終了
全シーン終了
未終了
符号化データの生成終了
GOPレイヤヘッダへの
暗号化された認証データの重畳
S5
GOPレイヤの符号生成・
パケット化・記憶装置504格納
S6
S7
全ピクチャ終了
全ピクチャ終了
未終了
ピクチャレイヤ符号化処理
S8

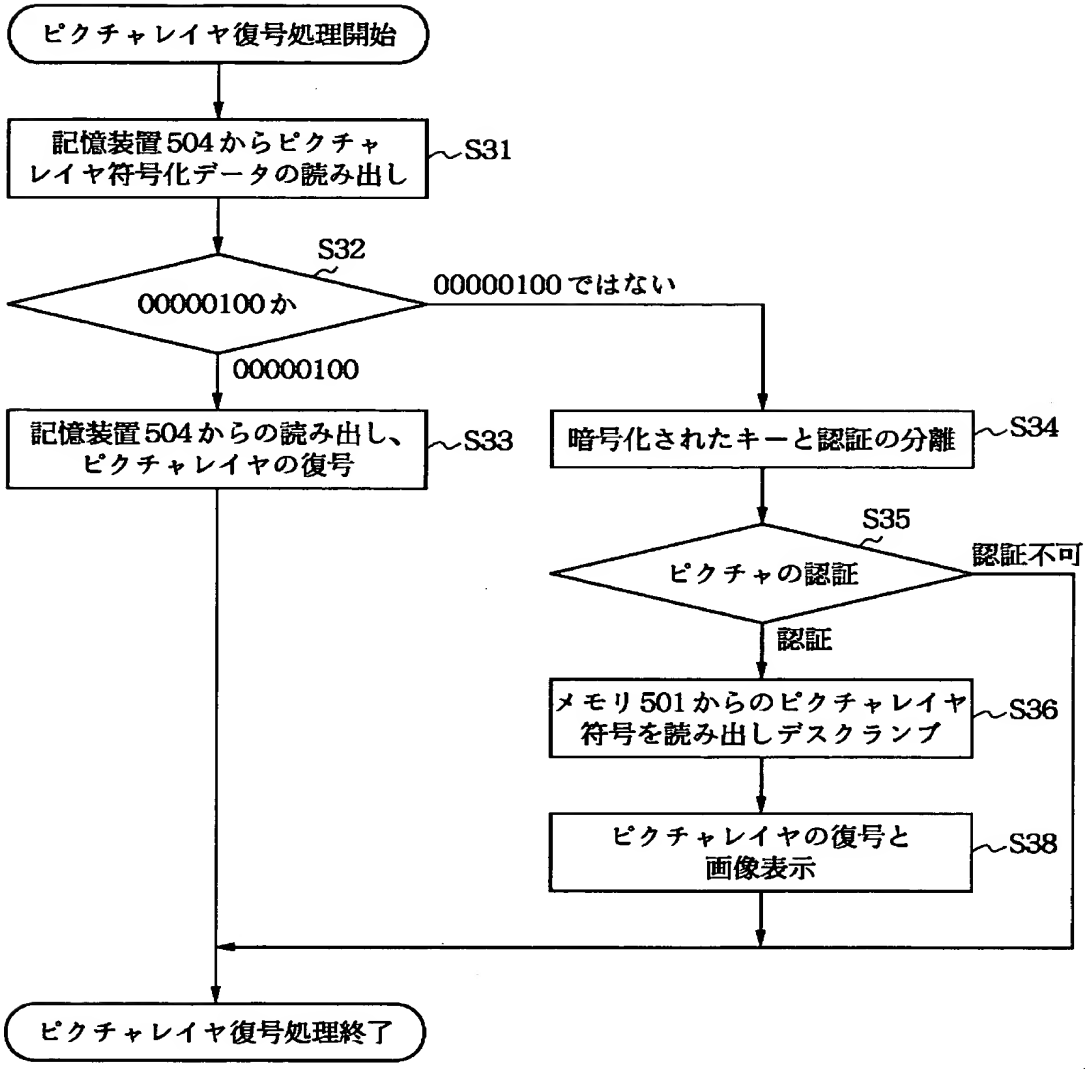
【図７】


ピクチャレイヤ符号化処理開始
S10
セキュリティの区間内
区間内
区間外
ピクチャレイヤの符号生成・
パケット化・記憶装置504格納
S11
ピクチャレイヤヘッダへの
暗号化されたキーと認証の重畳
S12
ピクチャレイヤの符号生成
S13
ピクチャレイヤの符号に
スクランブル
S14
ピクチャレイヤの符号生成・
パケット化・記憶装置504格納
S15
ピクチャレイヤ符号化処理終了

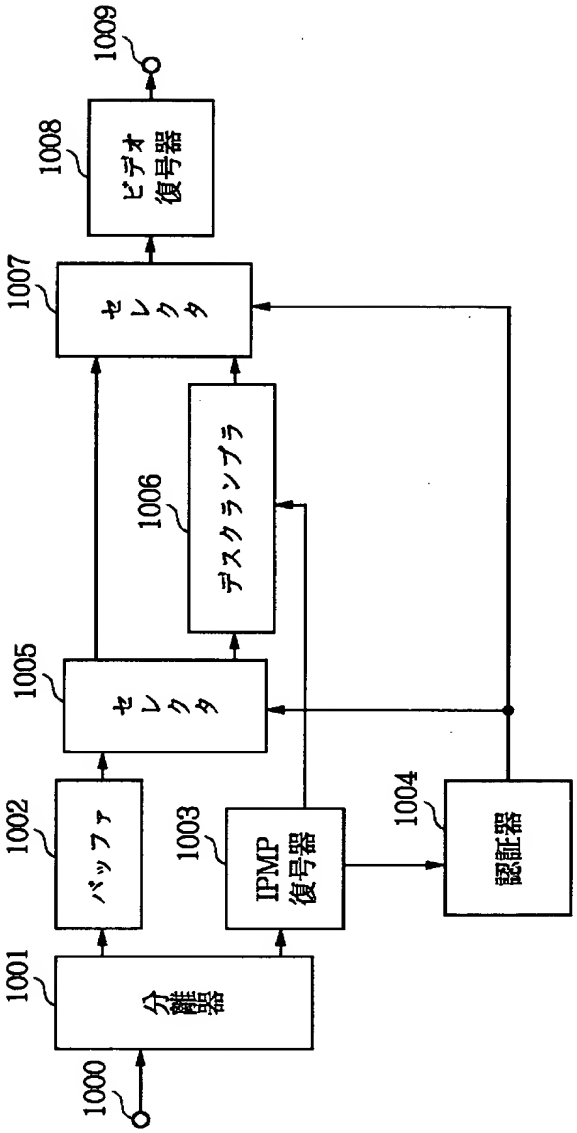
【図８】


符号化データの復号処理開始
記憶装置504から読み出し、
シーケンススタートコードの
分離、認証データの分離・解読
S20
S21
シーケンスレイヤの認証
認証不可
認証
シーケンスレイヤの復号
S22
S23
全GOP終了
全GOP終了
未終了
符号化データの復号処理終了
記憶装置504から読み出し、
GOPスタートコードの
分離、認証データの分離・解読
S24
S25
認証不可
GOPレイヤの認証
認証
GOPレイヤの復号
S26
S27
全ピクチャ終了
全ピクチャ終了
未終了
ピクチャレイヤ復号処理
S28

【図９】


ピクチャレイヤ復号処理開始
記憶装置504からピクチャレイヤ符号化データの読み出し
S31
S32
00000100か
00000100ではない
00000100
記憶装置504からの読み出し、ピクチャレイヤの復号
S33
暗号化されたキーと認証の分離
S34
S35
ピクチャの認証
認証不可
認証
メモリ501からのピクチャレイヤ符号を読み出しデスクランブ
S36
ピクチャレイヤの復号と画像表示
S38
ピクチャレイヤ復号処理終了

【図１０】


1009
1008
ビデオ復号器
1007
セレクタ
1006
デスクランブラ
1005
セレクタ
1002
バッファ
1003
IPMP復号器
1004
認証器
1001
分離器
1000

【図１１】


1010
BIFS符号化データ
1011
IPMP符号化データ
1012
ビデオ符号化データ
1013
オーディオ符号化データ

【図１２】

IPMP対象符号データ	ビデオ符号化データ
認証データ	nonac
セキュリティ対象	Frame No. 1～100　　解読キー yek
	Frame No. 1000～1260　　解読キー adeam

【書類名】　　要約書

【要約】

【課題】　冗長データの発生を抑えながら画像の著作権（知的財産）保護ができる画像処理を提供する。

【解決手段】　画像データを入力する入力端子１００と、前記画像データを保護するためのセキュリティデータを生成するセキュリティ設定器１０４と、前記画像データを符号化し、符号化データを生成するビデオ符号化器１０１と、前記セキュリティデータに従ってセキュリティが設定される区間の符号化データから一意に決定されるVOPスタートコードを抽出するスタートコード検出器１０５と、前記VOPスタートコードに前記セキュリティデータを重畳する暗号重畳器１０６と、前記セキュリティが設定された区間において前記VOPスタートコードを除いた前記符号化データにスクランブルを施すスクランブラ１０７と、暗号重畳器１０６によって処理されたスタートコードとスクランブラ１０７によって処理された符号化データとを出力する合成器１１１とを有する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００１００７〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社